Trabajo Fin de Grado

El Convenio sobre Ciberdelincuencia en el marco legal español.

Autor/es

Clara Sancho Va

Director/es

Carmen Tirado Robles

Universidad de Zaragoza
2016

INDICE:

GLOSARIO DE SIGLAS

1. CDPC: Comité Europeo del Consejo de Europa para los Problemas Criminares
2. CE: Constitución Española
3. CP: Código Penal
4. ISO: International Organization for Standardization (Organización Internacional de Normalización)
5. LO: Ley Orgánica
6. OCDE: Organización para la Cooperación y Desarrollo Económico
7. OMPI: Organización Mundial de la Propiedad Intelectual
8. PC-CY: Comité de Expertos en la Delincuencia del Ciberespacio
9. STC: Sentencia del Tribunal Constitucional
10. TIC: Tecnologías de la Comunicación y de la Información

I. INTRODUCCIÓN

La globalización, y en especial, la aparición y desarrollo de las Tecnologías de la Información y Comunicación (TIC a partir de ahora) han supuesto un avance decisivo no solo en nuestra vida cotidiana, sino también en las relaciones internacionales.

Todo ello trae causa del gran invento del siglo XX: Internet, que ha facilitado las relaciones sociales, y en general toda comunicación e intercambio de información anulando las posibles barreras (transfronterizas, geográficas…) que hasta ahora nos habían limitado. No obstante, este progreso ha supuesto también nuevas formas delictivas cuyo medio u objeto son los sistemas informáticos. Me refiero a la ciberdelincuencia, una nueva variedad de delitos sobre la que el legislador internacional se ha visto obligado a incidir.

Hasta el momento, el único instrumento internacional que regula dicha materia es el Convenio sobre Ciberdelincuencia del Consejo de Europa adoptado en Budapest el 23 de noviembre de 2001 (el Convenio a partir de ahora), objeto de mi Trabajo de Fin de Grado.

La razón por la que decidí centrarme en el estudio de esta norma, fue la originalidad de la materia, poder analizar y conocer cómo se está regulando una disciplina totalmente innovadora, puesto que, a diferencia de la mayoría de materias que son objeto de Derecho en las que el legislador se centra en realizar reformas sobre una base o contenido previo, el Convenio es un texto normativo totalmente innovador, no tiene antecedentes que regulen específicamente los delitos que en él se recogen. Lo único que podíamos encontrar hasta el momento eran determinadas conductas recogidas en textos normativos cuyo ámbito de aplicación solía ser el nacional, cuestión que me lleva a plantear otra de las razones por las que me interesó el Convenio: ver cómo el legislador hacía frente a una nueva dificultad: la indeterminación del ámbito geográfico.

Como antes he comentado, una de las principales ventajas que desde esta perspectiva se convierten en inconveniente, es la inexistencia de fronteras que permite al delincuente cometer un delito desde un Estado miembro en el cual no se encuentra la víctima, incluso llegando al extremo de desconocer desde qué lugar el infractor está actuando. Este hecho me generaba un gran número de dudas como qué órgano judicial

sería el competente para conocer del caso, qué Derecho le sería aplicable o cómo podemos asegurar la ejecución de la sentencia firme. Junto a ello, se le sumaba la posibilidad de que determinadas conductas fuesen punibles conforme al Derecho penal de un Estado miembro, pero no de otro creando de este modo, desigualdades en los derechos nacionales, zonas de impunidad, y en consecuencia, una grave inseguridad jurídica que perjudicaba especialmente al particular.

En conclusión, mi desconocimiento en todas estas cuestiones, junto con el interés que siempre he tenido en las nuevas tecnologías, fue lo que me permitió decidirme por estudio del Convenio sobre la ciberdelincuencia y su trasposición en la normativa española.

Con la finalidad de abordar dicho tema, decidí emplear, el método comparativo explicando en primer lugar lo que el Convenio establece para, posteriormente, determinar en qué grado el legislador español ha adoptado la norma en su regulación interna, ya que en más de una ocasión no se limita a plasmar la normativa sino que ve necesario ampliarla añadiendo por ejemplo circunstancias agravantes que no son reconocidas en el Convenio. No obstante, también hay supuestos donde el legislador, en vez de profundizar la normativa, ha creído conveniente simplificar la conducta delictiva.

Junto a ello, para poder profundizar más en el estudio también utilicé determinados textos normativos internacionales como la Convención sobre los Derechos del Niño, la Convención Europea de Derechos humanos, Protocolo Facultativo de la Convención de las Naciones Unidas sobre los Derechos del Niño relativo a la venta de niños, la prostitución infantil y la utilización de niños en la pornografía, Convenio Berna para la protección de obras literarias y artísticas etcétera.

Asimismo, también he utilizado en algunas ocasiones el método analítico, para poder conocer qué quiso decir el legislador con determinadas palabras que se encuentran en el precepto normativo. Por esta razón, no sólo tuve en cuenta el Convenio y el Código penal español, sino que empleé diversos materiales como el Informe explicativo del Convenio que me permitió poder entender con exactitud cuál era la finalidad del legislador internacional en cada artículo.

Por otra parte, en el ámbito nacional tuve que lidiar con una pequeña dificultad a la hora de encontrar información acerca de los artículos en los cuales se encuentran las

conductas castigadas por el Convenio, puesto que la Reforma del Código penal de diciembre de 2015 tuvo una gran incidencia sobre los delitos cibernéticos, ampliando y concretando el contenido de los mismos.

Todo ello con la finalidad de poder recabar información suficiente para que quedase un trabajo completo, que no diese lugar a dudas o lagunas de contenido.

No obstante, para poder iniciar la investigación, decidí partir de la historia del Convenio, comentando las razones que instaron al Consejo de Europa a legislar sobre esta materia.

II. EVOLUCIÓN HISTÓRICA DEL CONVENIO SOBRE CIBERDELINCUENCIA

1. LA HISTORIA DEL CONVENIO

El Convenio sobre Ciberdelinuencia[1] adoptado en Budapest el 23 de noviembre de 2001 del Consejo de Europa, surgió frente a la gran amenaza que Internet implica: los daños transfronterizos. Es decir, la posibilidad de causar daños internacionales, existiendo una disociación entre el lugar desde el que se causa el daño y el lugar donde se localiza el resultado de ese daño. En él se establece la base de una política penal internacional que permita proteger a los usuarios de sistemas informáticos, de la ciberdelincuencia.

Esta norma es, hasta el momento, el primer y único convenio en materia de ciberdelincuencia. Por ello, es relevante estudiar los orígenes y evolución del mismo.

La primera actuación que se realizó en esta materia fue en noviembre de 1996, cuando el Comité europeo del Consejo de Europa para los problemas criminales (CDPC) determinó en la decisión CDPC/103/211196 la creación de un comité de expertos en materia de delitos informáticos.

[1]Convenio sobre Ciberdelincuencia. BOE: http://www.boe.es/diario_boe/txt.php?id=BOE-A-2015-793

No obstante, encontramos autores como Rodríguez Bernal [2], que sitúan el verdadero origen del Convenio en 1983, momento en el que un grupo de expertos formado por miembros de numerosos organismos internacionales como Interpol, la Organización de Naciones Unidas y la Unión europea entre otros, advierte a la Organización para la Cooperación y Desarrollo Económico (OCDE) de la inminente necesidad de elaborar un sistema de cooperación internacional en el que se tratase la materia de delitos informáticos. Consecuentemente, se elaboró un informe en 1986[3] que sirvió para que el Consejo de Europa publicase una Recomendación en el año 1989[4], siendo el punto de partida para las negociaciones que culminaron en Budapest en 1996.

Las razones por las cuales se llegó a la decisión CDPC/103/211196, dejando a un lado la mencionada apreciación del autor Rodríguez Bernal, fueron varias: la aparición del ciberentorno[5], la facilidad de almacenamiento y transmisión de todo tipo de información y documentos, la sencillez a la hora de conectarse con diversas partes del mundo a través de una pantalla... No obstante, todas ellas tienen en su origen, una misma causa: el rápido avance de las nuevas tecnologías.

Se trata de un ámbito que todavía sigue siendo desconocido y el cual podía y puede ser usado con fines ilegítimos al atacar o dañar la integridad, la confidencialidad o la disponibilidad de la información que guardan los sistemas de telecomunicaciones. Junto a ello, se tuvo en cuenta un factor muy importante: la naturaleza ilimitada y transfronteriza de las nuevas tecnologías, haciendo posible que el delito se ejecute en un país diferente del que se ha originado.

Por ello el CDPC destacó la necesidad de realizar un esfuerzo por parte de todos los Estados para aunar una base normativa que solventase ambos problemas: la comisión de delitos informáticos y, consecuentemente, los posibles conflictos de

[2]RODRIGUEZ BERNAL, A. "Los Cibercrímenes en el Espacio de Libertad, Seguridad y Justicia" en *Revista de derecho informático*, nº 103, 2007, pág 13.
[3]Computer-related Crime: Analysis of Legal Policy
[4] Recomendación del Consejo de Europa año 1989. Consejo de Europa: https://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/ETS%20185%20Explanatory%20report_Spanish.pdf
[5]Ciberentorno: incluye a usuarios, redes, dispositivos, todo el software, procesos, información almacenada o que circula, aplicaciones, servicios y sistemas que están conectados directa o indirectamente a las redes: JIMÉNEZ GARCÍA, F., "La ciberseguridad en el marco internacional. El Convenio de Budapest de 2001 sobre la Ciberdelincuencia adoptado en el Consejo de Europa" *La protección y seguridad de la persona en internet: aspectos sociales y jurídicos*, JORDA CAPITAN E. .R, et al.(coord.), 2014, Scientia Iuridica. Págs. 49 y ss

territorialidad que podían surgir. Llegados a este punto, el CDPC pidió a H. W. K. Kaspersen, un experto internacional en criminología, que realizase un informe[6] sobre la situación del mundo cibernético en aquel momento y la posibilidad de establecer una regulación internacional. En dicho informe se argumentaba que la forma más conveniente de realizar una regulación era redactando un convenio, ya que los restantes instrumentos jurídicos no aportarían la fuerza vinculante característica de esta fuente normativa. Asimismo, añadió que dicho convenio no solo debía tratar la materia en el Derecho penal sustantivo, sino que también debería establecer unas pautas en cuanto al Derecho procesal penal y la cooperación internacional.

Unos meses más tarde, concretamente el 4 de febrero de 1997, tuvo lugar una reunión de ministros del Consejo de Europa, en la que se creó el "Comité de Expertos en la Delincuencia del Ciberespacio" (PC-CY).El Comité PC-CY comenzó a trabajar en el proyecto de un convenio sobre la cibercriminalidad en abril de ese mismo año, debiendo terminar antes del inicio del año 2000, sin embargo fue en junio del 2001 cuando el Comité de Ministros dio su aprobación y como consecuencia quedó abierto para su firma.

Desde abril de 1997 hasta diciembre del 2000, se fueron realizando las actuaciones correspondientes, entre las que cabe mencionar las 10 reuniones plenarias del Comité PC-CY y 15 reuniones de su Grupo de Redacción. En todas ellas, las negociaciones fueron arduas y complejas, de hecho, en este periodo de tiempo se llegaron a redactar hasta treinta versiones del proyecto. Los ministros de Justicia europeos apoyaron en más de una ocasión (Praga, junio de 1997 y Londres junio del 2000 entre otros), la labor que estaba llevando a cabo el Comité de Expertos en la Delincuencia del Ciberespacio, alentándolos a continuar con el proyecto con dos objetivos primordiales: poder solventar de un modo rápido y eficiente los problemas derivados de la ciberdelincuencia y poder conseguir que fuese firmado y ratificado por el mayor número de Estados. Pero este apoyo no fue simplemente mostrado por los ministros de Justicia de la Unión Europea, sino que a ello también se le sumó el recibido

[6]Informe: *Implementation of Recommendation Nº R (89)9on computer related crimes. Doc. CDPC (97) 5 y PC-CY (97) 5*, 1990.

por parte de sus Estados miembros, el cual se encuentra recogido en una Opinión Conjunta adoptada en el año 1999[7].

A principios del año 2000, se concertaron tres reuniones adicionales con el objetivo de finalizar el proyecto y estudiarlo de nuevo, pero con una diferencia: esta vez se daría a conocer en la Asamblea Parlamentaria y ésta, daría su opinión sobre el mismo.

Concretamente, fue el 27 de abril de 2000 cuando se alcanzó el consenso necesario para poder publicar el Proyecto de Convenio sobre Delito Cibernético, no obstante, esta primera versión no prosperó. A partir de este momento, se fueron realizando diversas versiones del Proyecto. Esto dio la oportunidad a los Estados negociadores de poder solventar todas aquellas cuestiones que el mismo les pudiese suscitar, hecho que resultó muy favorable en el momento de ratificar el convenio por parte de estos Estados.

Medio año más tarde, en octubre de 2000, el Comité de Ministros solicitó a la Asamblea la emisión de un dictamen en el que se pronunciase acerca del mencionado proyecto, el cual no fue adoptado hasta abril de 2001, coincidiendo con la segunda sesión plenaria de la Asamblea Parlamentaria del Consejo de Europa.

Finalmente, el Convenio sobre la Ciberdelincuencia fue aprobado por el Consejo de Ministros del Consejo de Europa el 8 de noviembre de 2001 y 15 días más tarde, es decir el 23 de noviembre, abierto para su firma.

2. ESTADO ACTUAL DEL CONVENIO SOBRE CIBERDELINCUENCIA

Actualmente el Convenio sobre la Ciberdelincuencia ha sido firmado por un total de 55 países[8], no siendo ratificado por seis de los mismos: Andorra, Grecia, Irlanda, Mónaco, Suiza y Sudáfrica.

[7]Posición Común 199/364/JAI, de 27 de mayo de 1999 adoptada por el Consejo de la Unión Europea sobre la base del artículo 34 del Tratado de la Unión Europea, relativa a las negociaciones del proyecto de Convenio sobre delincuencia en el ciberespacio celebradas en el Consejo de Europa. DOUE L 142/1 de 5. 6. 1999.

[8]Tabla de Estados Miembros del Convenio sobre Ciberdelincuencia. Anexo I y II: http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures

España, fue uno de los países que estuvo presente desde las negociaciones iniciales del Convenio. Este hecho, junto a la pertenencia al Consejo de Europa hizo que nuestro país firmase el convenio nada más ser aprobado. No obstante, no fue hasta junio de 2010 cuando España decidió ratificarlo. Junto con el instrumento de ratificación[9], nuestro gobierno realizó tres declaraciones:

En primer lugar, hizo referencia a Gibraltar, un territorio no autónomo de cuyas relaciones exteriores es responsable Reino Unido, y el cual se encuentra inmerso en un conflicto bilateral con el Reino Unido. Aquí, el Estado español quiso destacar que la eventual participación de las autoridades gibraltareñas en la aplicación del Convenio, se entendería realizada exclusivamente en el marco de las autoridades gibraltareñas internas, quienes tienen su origen y fundamento en la distribución y atribución de competencias efectuadas por el Reino Unido. Estas observaciones realizadas por parte del Estado Español, tienen su fundamento en las controversias políticas que España vive con Reino Unido.

En segundo lugar declaró que la autoridad central designada, a la que hacen referencia los artículos 24 y 27 del Convenio, es decir, la autoridad responsable del envío o recepción de solicitudes de extradición o de detención provisional en ausencia de un tratado y la autoridad encargada de enviar la solicitud de asistencia mutua de su ejecución y de su remisión sería la Subdirección General de Cooperación Jurídica Internacional del Ministerio de Justicia.

Finalmente, también estableció que sería la Comisaría General de Policía Judicial del Ministerio de Interior la que, conforme al artículo 35 del Convenio, adoptaría la figura de punto de contacto disponible para la prestación de ayuda inmediata para los fines de las investigaciones y procedimientos relacionados con delitos informáticos.

Por otra parte, también merece una especial referencia la evolución de los Estados no miembros del Consejo de Europa realizada en los últimos cuatro años, puesto que desde que se aprobó el Convenio, tan solo había sido ratificado por Estados Unidos. Sin embargo, como muestra la tabla, a partir de 2012, fueron varios (concretamente siete de ocho) los Estados terceros que decidieron ratificarlo.

[9]Instrumento de ratificación. BOE: https://www.boe.es/diario_boe/txt.php?id=BOE-A-2010-14221

Concretamente, fueron Australia y Japón quienes ratificaron este marco normativo en el año 2012, seguidos de República Dominicana y Mauricio en el 2013. Posteriormente el año 2014 Panamá decidió dar este paso, siendo los últimos países en adherirse Sri Lanka y Canadá en el año 2015. Actualmente Argentina está estudiando la posibilidad de ratificar el Convenio.

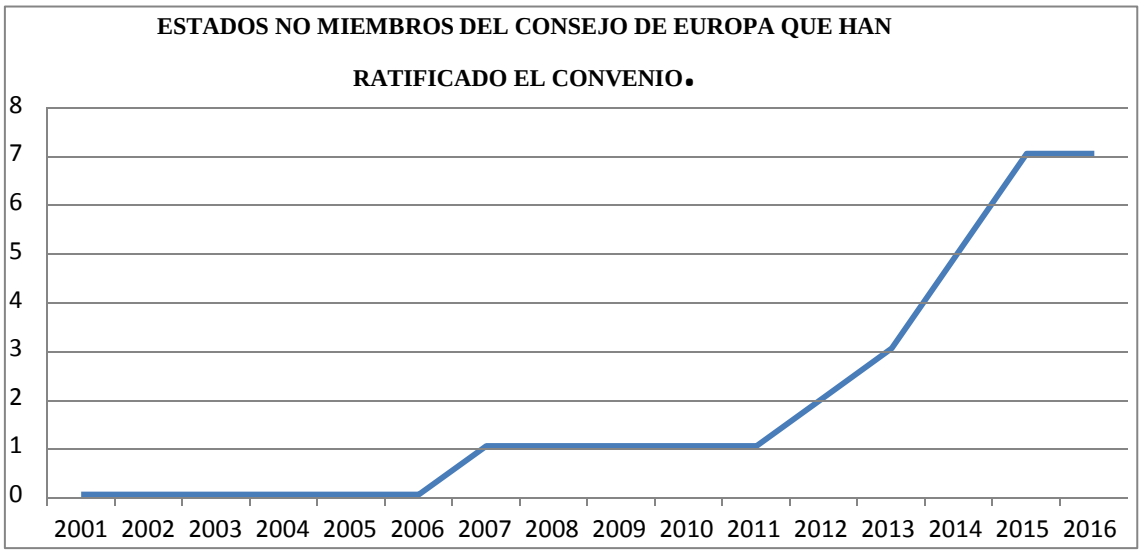

Figura 1. Relación del número de estados terceros que han firmado el convenio, con la fecha en la que lo realizaron. Fuente de elaboración propia.

3. EL PROTOCOLO ADICIONAL AL CONVENIO SOBRE LA CIBERDELINCUENCIA

Llegados a este punto, es importante que tengamos en cuenta un instrumento que se redactó como complemento al Convenio en el año 2003: *El Protocolo adicional al Convenio sobre la ciberdelincuencia relativo a la penalización de actos de índole racista y xenófoba cometidos por medio de sistemas informáticos* [10] adoptado en Estrasburgo el 30 de enero de 2003.

Con este documento se amplió el elenco de delitos relacionados con el contenido regulados en el Titulo 3 del Convenio (concretamente artículo 9: Delitos relacionados con la pornografía infantil), cometidos a través de sistemas informáticos, tratando los mismos aspectos que el Convenio sobre Ciberdelincuencia: terminología, aspectos

[10]Protocolo adicional al Convenio sobre la ciberdelincuencia relativo a la penalización de actos de índole racista y xenófoba cometidos por medio de sistemas informáticos. BOE: https://www.boe.es/diario_boe/txt.php?id=BOE-A-2015-793

penales, procesales y la cooperación internacional. La finalidad última de este texto normativo, apreciada en su Preámbulo, era la necesidad de una respuesta jurídica completa y concreta a los actos de propagación de índole racista y xenófoba divulgada a través de los medios informáticos. Para ello, este cuerpo legal adopta las correspondientes medidas penales contra la difusión de material racista y xenófobo mediante sistemas informáticos, compeliendo a los Estados Miembros a tipificar como delitos graves las amenazas realizadas a personas por razón de raza, color, etnia, así como por su religión tal y como indica en sus artículos 3 y 4.

Asimismo, establece en su artículo 6 la necesaria tipificación de todos aquellos actos cometidos voluntaria y conscientemente que impliquen la difusión o publicación de todo aquel material que niegue, minimice, apruebe o justifique los genocidios o crímenes contra la humanidad.

Pero, pese a la brevedad del texto, la elaboración no resultó sencilla. Surgió una dificultad añadida vinculada a la materia que se regula: la libertad de expresión, fundamento esencial de una sociedad democrática y pilar primordial para el progreso y la evolución del ser humano. Se trataba de regular un ámbito que choca con el principio de libertad de expresión. Esta es la principal razón por la que el Protocolo establece criterios generales, amplios y flexibles, remitiendo en un gran número de ocasiones a la legislación interna de los Estados Miembros.

Dicho protocolo entró en vigor el 1 de marzo de 2006 y consecuentemente desde la fecha, completa la materia del Convenio de Budapest.

III. ASPECTOS GENERALES DEL CONVENIO

El contenido del Convenio sobre Ciberdelincuencia, se encuentra dividido en cuatro grandes bloques, dando lugar cada uno de ellos a un capítulo. En el primero (artículo 1), bajo la rúbrica *Terminología* se encuentran recogidos una serie de conceptos y definiciones esenciales para aplicación del Convenio. En segundo lugar encontramos el capítulo: *Medidas que deberán adoptarse a nivel nacional*, recogido en los artículos 2 a 22 del texto. Este capítulo se divide a su vez en tres secciones: Derecho penal sustantivo, Derecho procesal y Jurisdicción. Posteriormente el tercer capítulo se

centra en la *Cooperación internacional* (artículos 23 a 45). El Convenio se cierra con un último capítulo denominado *Disposiciones finales* (artículos 36 a 48 del Convenio).

1. TERMINOLOGÍA

El Convenio comienza fijando unos conceptos comunes, con la finalidad de distinguir los siguientes términos: sistema informático, datos informáticos, proveedor de servicios y datos sobre el tráfico. Se trata de unos conceptos esenciales para la correcta aplicación del Convenio.

Concretamente en el primer apartado del artículo 1, establece que "Por «sistema informático» se entenderá todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, siempre que uno o varios de ellos permitan el tratamiento automatizado de datos en ejecución de un programa". En este aspecto, es importante incidir en determinados conceptos. El más relevante en este primer apartado sería "dispositivo" con el que no solo se hace referencia al soporte físico (también conocido como hardware), sino también a todos los programas informáticos[11], datos y aplicaciones que el mismo contenga (software). Además, también debe otorgarse cierta relevancia al concepto "automatizado", es decir, aquel dispositivo que puede trabajar sin intervención del ser humano.

En el segundo apartado del artículo 1, encontramos el concepto de «datos informáticos», entendido como "cualquier representación de hechos, información o conceptos de una forma que permita el tratamiento informático, incluido un programa diseñado para que un sistema informático ejecute una función", es decir, datos que permitan un directo procesamiento informático. Dicho concepto se basó en una definición de la palabra “datos” realizada por la International Organization for Standardization, también conocida como Organización Internacional de Normalización (ISO a partir de ahora) y podría considerarse doblemente importante, porque por una parte, todas las conductas tipificadas en esta norma se resumen en un ilegal e incorrecto uso, obtención o tenencia de datos informáticos, y, porque por otra, estos datos informáticos constituyen también el objeto de las medidas de investigación que los Estados miembro pueden solicitar con el fin de cooperar entre ellos.

[11] Programa informático: conjunto de instrucciones que pueden ser ejecutadas por el equipo para alcanzar un resultado deseado.

Siguiendo en la misma línea de aclaración y concreción de la terminología utilizada, el artículo 1.3 del Convenio determina qué se debe entender por "proveedor de servicios", distinguiendo dos posibilidades: "A) Toda entidad pública o privada que ofrezca a los usuarios de sus servicios la posibilidad de comunicar por medio de un sistema informático, y B) cualquier otra entidad que procese o almacene datos informáticos para dicho servicio de comunicación o para los usuarios de ese servicio". Como se puede observar, este concepto comprende una extensa variedad de entidades cuyo objeto es el procesamiento de datos mediante sistemas informáticos, sin importar su naturaleza jurídica, ni el destinatario de los servicios ya que puede ser que los usuarios sean grupos cerrados, o que directamente el proveedor ofrezca sus servicios al público.

Finalmente, el artículo 1 se cierra con la definición de "datos sobre el tráfico", entendidos como "cualesquiera datos informáticos relativos a una comunicación por medio de un sistema informático, generados por un sistema informático como elemento de la cadena de comunicación, que indiquen el origen, destino, ruta, hora, fecha, tamaño y duración de la comunicación o el tipo de servicio subyacente". Por lo tanto, es imprescindible establecer una clara distinción entre datos informáticos y datos sobre el tráfico, teniendo en cuenta que estos últimos están sujetos a un régimen jurídico específico y que, principalmente, son necesarios para diversas tareas de investigación como puede ser rastrear el origen de una comunicación como punto de partida para reunir otras pruebas.

2. OBLIGACIONES Y FORMAS DE RESPONSABILIDAD

En este capítulo, se establece el deber de los Estados de adoptar las medidas tanto legislativas como de cualquier otro tipo que resulten necesarias para poder tipificar las conductas recogidas en el Convenio en su Derecho interno[12]. Los delitos recogidos

[12] Artículo 13: Sanciones y medidas
1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para que los delitos previstos de conformidad con los artículos 2 a 11 puedan dar lugar a la aplicación de sanciones efectivas, proporcionadas y disuasorias, incluidas penas privativas de libertad.
2. Cada Parte garantizará la imposición de sanciones o de medidas penales o no penales efectivas, proporcionadas y disuasorias, incluidas sanciones pecuniarias, a las personas jurídicas consideradas responsables de conformidad con el artículo 12.

en el texto legal son la base, pero ello no indica que los Estados no puedan ampliar el elenco de acciones u omisiones recogidas o los modos de cometer la conducta.

Además, el Convenio en su artículo 11 realiza una precisión en materia de responsabilidad, previendo que los Estados parte no solo hagan responsables a los autores, sino que también reconozcan la responsabilidad, y por lo tanto sean sancionados, los actos de complicidad y tentativa. Concretamente, el artículo 11 en su primer apartado, establece que los Estados tomarán las medidas necesarias para tipificar como delito la complicidad intencionada de los delitos recogidos en los artículos 2 a 10 del Convenio. Asimismo, en su segundo apartado establece el deber de adoptar las medidas necesarias para tipificar como delito cualquier tentativa de comisión de los delitos recogidos en los artículos 3 a 5, 7, 8, 9.1 a) y c).

Junto a ello se debe mencionar la responsabilidad de las personas jurídicas, la cual se encuentra recogida en el artículo 12 del mismo cuerpo legal, donde se establece que cuando una persona física en virtud de: a) un poder de representación de la persona jurídica; b) una autorización para tomar decisiones en nombre de la persona jurídica; o c) una autorización para ejercer funciones de control en la persona jurídica realice una conducta tipificada en el presente Convenio, se le podrá exigir responsabilidad penal, sin importar si la persona física obraba en calidad individual o en condición de miembro de un órgano de dicha persona jurídica.

Esto debe completarse con el apartado segundo del mismo artículo, donde se establece que cada Estado deberá adoptar las medidas necesarias para asegurar la posibilidad de exigir responsabilidad a una persona jurídica cuando la falta de vigilancia o de control por parte de una persona física que cumple alguna de las condiciones del primer apartado haya hecho posible la comisión de un delito previsto en el Convenio.

IV. EL CONVENIO SOBRE CIBERDELINCUENCIA EN LA LEGISLACIÓN ESPAÑOLA.

1. DERECHO PENAL SUSTANTIVO:

El Convenio distingue los delitos dependiendo del bien jurídico protegido, de este modo encontramos: *Los delitos contra la confidencialidad, la integridad y la*

disponibilidad de los datos y sistemas informáticos, los delitos informáticos, los delitos relacionados con el contenido y *los delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines.*

Sin embargo, el Código penal español[13] no solo no adopta esta sistemática sino que ni si quiera tiene un capítulo concreto en el que trate la materia de los delitos cibernéticos, a diferencia por ejemplo del Código penal francés que contiene capítulos concretos cuyo bien jurídicamente protegido es la seguridad en los sistemas informáticos.

Llegados a este punto, debemos poner de relieve una cuestión relativa a la determinación del bien jurídico protegido que mantiene a la doctrina española dividida. Por una parte encontramos la vertiente más clásica, que identifica el bien protegido con el daño a la propiedad ajena, afirmando que por el hecho de que estos delitos sean cometidos mediante o contra sistemas informáticos no adquieren una naturaleza diferente. La doctrina moderna sin embargo, critica esta interpretación confirmando la existencia de un nuevo bien jurídico supraindividual que debe ser objeto de protección penal. Se trata de un bien jurídico que todavía no ha sido concretamente determinado, pero que giraría en torno a la seguridad de los sistemas informáticos y las redes de telecomunicación[14].

A pesar por lo tanto de la inexistencia de un capítulo donde se recojan los delitos informáticos, no se debe menospreciar la proposición relativa a la agrupación de éstos bajo el título de "delitos contra la seguridad en los sistemas de información". Proposición previa a la Reforma del Código Penal de 2015, que hasta ahora no ha sido tenida en cuenta por el legislador. Entiendo que esta omisión puede deberse a un desacuerdo respecto a la actual estructura del Código Penal, la cual no facilita la creación de un capítulo exclusivo dedicado a los delitos informáticos, ya que en muchas ocasiones el legislador ha preferido introducir un nuevo modo de cometer el delito (a través de sistemas informáticos), en vez de crear uno nuevo. Un ejemplo de ello podría ser el delito de estafa informática, donde el legislador ha incorporado un nuevo precepto (artículo 248.2 Código Penal) en el que determina que también se considera estafa la acción de manipular mediante sistemas informáticos un dato con la finalidad de obtener

[13] Código penal español. BOE: https://www.boe.es/buscar/act.php?id=BOE-A-1995-25444
[14] GONZALEZ HURTADO, J.A., "Delincuencia informática: Daños informáticos del artículo 264 del Código Penal y propuesta de reforma", Universidad Complutense de Madrid, Madrid, 2013.

una transferencia no consentida de cualquier activo patrimonial, en lugar de crear un nuevo delito que pueda incorporarse en un capítulo como el propuesto.

1.1. Los delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos

Estas conductas se encuentran recogidas en los artículos 2 a 6 del Convenio. Llegados a este punto se debe tener en cuenta la Directiva 2013/40/UE del Parlamento Europeo y del Consejo de 12 de Agosto de 2013 relativa a los ataques contra los sistemas de información y por la que sustituye la Decisión marco 2005/222/JAI del Consejo de la Unión Europea de 24 de febrero[15]. Durante la redacción del Convenio, la Decisión marco 2005/222/JAI del Consejo de la Unión Europea de 24 de Febrero relativa a los ataques contra los sistemas de información[16] se consideró necesaria debido a los posibles ataques que podrían llevar a cabo organizaciones criminales y grupos terroristas contra sistemas informáticos de instituciones vitales para los Estados miembros, poniendo en peligro según dicho texto normativo, la realización de una sociedad de la información segura y de un espacio de libertad, seguridad y justicia. No obstante, debemos tener en cuenta que esta Decisión Marco fue sustituida por la Directiva 2013/40/UE (la Directiva a partir de ahora), nueva regulación que apenas presenta diferencias relevantes con respecto al texto que sustituye.

En ella se incorpora un primer artículo relativo al objeto, donde determina que en el articulado de la Directiva no solo se van a establecer unas normas mínimas concernientes a la definición de las conductas penales y sanciones aplicables, sino que también tiene como finalidad poder facilitar la prevención de dichas infracciones y la mejora en el ámbito de la cooperación entre las autoridades competentes.

Además, del mismo modo que su texto normativo referente, la Directiva establece que los Estados miembros deben adoptar las medidas necesarias para la tipificación penal de delitos como el acceso ilegal a los sistemas de información, interferencia ilegal en los sistemas de información e interferencia ilegal en los datos. Anteriormente, la Decisión Marco 2005/222/JAI, hacía referencia a los mismos delitos

[15] Directiva 2013/40/UE del Parlamento Europeo y del Consejo de 12 de Agosto de 2013 relativa a los ataques contra los sistemas de información y por la que sustituye la Decisión marco 2005/222/JAI del Consejo de la Unión Europea de 24 de febrero. BOE: https://www.boe.es/doue/2013/218/L00008-00014.pdf

[16] Decisión marco 2005/222/JAI del Consejo de la Unión Europea de 24 de Febrero relativa a los ataques contra los sistemas de información. BOE: https://www.boe.es/doue/2005/069/L00067-00071.pdf

pero con denominaciones distintas, no obstante, el contenido de la norma no ha sido modificado. Sin embargo, la Directiva sí que ha introducido un nuevo tipo delictivo en su artículo 6: "la interceptación ilegal" donde se castiga la interceptación por medios técnicos de transmisiones no públicas.

Junto a ello, debemos poner de relieve la supresión del artículo en el que se obligaba a observar una circunstancia agravante en el caso de que el delito hubiera sido cometido en la sede de una organización criminal, no obstante ahora en su Considerando 19 tan solo se establece que los Estados deberán prever circunstancias agravantes que tendrán que ser conocidas por los jueces.

Finalmente, en lo que a modificaciones se refiere, también debemos mencionar el nuevo artículo 7 relativo a los instrumentos utilizados para cometer infracciones. En él se establece que los Estados deberán sancionar aquellas conductas tendentes a poner en disposición de un tercero cualquier material que permita realizar los delitos recogidos en la presente Directiva.

No obstante, una parte muy importante del contenido de este texto normativo ha permanecido intacta. Me refiero principalmente a la forma de responsabilidad que, hasta la interposición de la Decisión Marco 2005/222/JAI no era contemplada por el Convenio: la inducción. Además también se incide sobre la complicidad y tentativa, así como la responsabilidad de las personas jurídicas.

Todas estas medidas permiten responder con una mayor eficacia a esas posibles amenazas, tal y como se puso de manifiesto en la Comunicación de la Comisión titulada: "Seguridad de las redes y de la información: Propuesta para una perspectiva política europea."[17], además de acercar las legislaciones nacionales en la materia regulada.

En definitiva, esta Directiva supuso un avance para la regulación establecida en el Convenio, no tanto desde la perspectiva de las conductas tipificadas, pero si desde el punto de vista de las medidas legislativas sobre las que los Estados miembro debían trabajar y las formas de responsabilidad reconocidas hasta entonces.

Identificando ya cada una de las conductas delictivas en este área, la primera que recoge el Convenio en su artículo 2 es la denominada: acceso ilícito, es decir, "el acceso

[17]DO C 300 E de 11.12.2003 p.26

deliberado e ilegítimo a la totalidad o a una parte del sistema informático". Con ella se pretende proteger los intereses tanto de las organizaciones como de las personas con la finalidad de que puedan manejar, operar y controlar sus sistemas informáticos sin interrupción ni restricción alguna. Esta conducta la encontramos actualmente tipificada en el art 197 bis del Código Penal[18] (CP) añadida por el artículo único 107 de la reciente L.O. 1/2015, de 30 de marzo, por la que se modifica la L.O. 10/1995, de 23 de noviembre, del Código Penal[19]. El artículo 197 bis 1 recoge la conducta anteriormente establecida en el artículo 197.3 CP[20] sustituyendo el concepto de autorización por el de consentimiento. Sin embargo, a pesar de las reformas introducidas en este precepto, el legislador español ha optado por mantener la exigencia de vulnerar un sistema de seguridad, para que la conducta realizada se pueda subsumir al tipo delictivo regulado.

En el Informe explicativo del Convenio[21] se establece que se considerará acceso ilícito la mera intromisión no autorizada a una parte o a la totalidad del sistema informático. Luego con esta conducta, ambos cuerpos legales (el Convenio y el Código Penal) están castigando la piratería, el sabotaje y la intrusión en el ordenador, es decir, el *hacking*, *cracking* y *computer trespass*, puesto que todas ellas son un impedimento para los dueños legítimos de los datos y sistemas.

En relación con este primer tipo, se encuentra recogida en el artículo 3 del Convenio la conducta relativa a la interceptación ilícita, entendida como una interceptación deliberada e ilegítima de datos informáticos privados realizada a través

[18]Artículo 197 bis CP

1. "El que por cualquier medio o procedimiento, vulnerando las medidas de seguridad establecidas para impedirlo, y sin estar debidamente autorizado, acceda o facilite a otro el acceso al conjunto o una parte de un sistema de información o se mantenga en él en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, será castigado con pena de prisión de seis meses a dos años.
2. El que mediante la utilización de artificios o instrumentos técnicos, y sin estar debidamente autorizado, intercepte transmisiones no públicas de datos informáticos que se produzcan desde, hacia o dentro de un sistema de información, incluidas las emisiones electromagnéticas de los mismos será castigado con una pena de prisión de tres meses a dos años o multa de tres a doce meses".

[19]L.O. 1/2015, de 30 de marzo, por la que se modifica la L.O. 10/1995, de 23 de noviembre, del Código Penal. BOE: https://www.boe.es/diario_boe/txt.php?id=BOE-A-2015-3439

[20]Artículo 197.3 CP previo a la reforma de 2015:

"El que por cualquier medio o procedimiento y vulnerando las medidas de seguridad establecidas para impedirlo, acceda sin autorización a datos o programas informáticos contenidos en un sistema informático o en parte del mismo o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, será castigado con pena de prisión de seis meses a dos años."

[21]Informe explicativo del Convenio:
https://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/ETS%20185%20Explanatory%20report_Spanish.pdf

de sistemas de telecomunicación[22]. La finalidad de este tipo delictivo es la protección del derecho a la privacidad en los sistemas informáticos, cuyo fundamento se encuentra en el artículo 8 de la Convención Europea de Derechos Humanos[23], que establece el derecho al respeto a la vida privada y familiar.

Esta conducta también ha sido recientemente incorporada en nuestra legislación en el artículo 197 bis 2 mediante el ya mencionado artículo único 107 de la L.O. 1/2015[24], reconocida por parte de la doctrina entre la que figura el Magistrado Don Eloy Velasco Nuñez, como un delito de allanamiento informático, el cual requiere un dolo reduplicado, puesto que no solo se debe tener la finalidad de acceder a un sistema informático ajeno sin autorización expresa, sino que se suma también la necesidad o intención de vulnerar las claves de protección impuestas al sistema para acceder a éste[25]. Es decir, con esta conducta lo que se quiere proteger no es solo la propiedad de los documentos que hay en el sistema, sino también el modo de acceso al mismo.

Además, debe tenerse en cuenta que el legislador español ha introducido una novedad en el artículo 197 quater respecto de los delitos hasta ahora estudiados, aplicando penas superiores en grado a quienes hubieran cometido estos delitos en el seno de una organización o grupo criminal.

Asimismo, también está tipificada en el artículo 4 del Convenio la interferencia en los datos, esto es, "(...) la comisión de forma deliberada e ilegítima de actos que dañen, borren, deterioren, alteren o supriman datos informáticos". Con este delito lo que se pretende es poder otorgar una protección a los datos y programas informáticos similar a la que tienen los objetos tangibles, es decir, proteger la integridad y el correcto funcionamiento de los datos y programas informáticos.

En España, a diferencia de la norma internacional, esta conducta no la tenemos regulada a continuación de los delitos de acceso e interferencia ilícita, sino que debemos acudir al artículo 264 CP. En dicho artículo encontramos una exacta trasposición de las

[22]JIMÉNEZ GARCÍA, F., *La ciberseguridad en el marco internacional..., cit.. p.67*
[23]Convención Europea de Derechos Humanos: http://www.echr.coe.int/Documents/Convention_SPA.pdf
[24] Artículo único 107 de la L.O. 1/2015. Fuente: https://www.boe.es/diario_boe/txt.php?id=BOE-A-2015-3439
[25] ELOY VELASCO, E. "*Los delitos informáticos*". Artículo monográfico. Diciembre 2015: http://www.sepin.es/abogado-penalista/VerDoc.asp?referencia=SP%2FDOCT%2F19492&cod=0JP1yG1S_0Ha17U1DT0Fa1eq0XP0Fk1vl0H60Fa1dB0H50Ha1%3DK0Vl0Fa17P0GD0G_1AS1yt0FF1Mu1Cq0GA1FA00u0E_1Mt1Dv09P1C50GF0Cp0yf00v#23984238

acciones recogidas en la norma internacional que, pese a las proposiciones de reducir y sustituir la conducta contenida en nuestra legislación por la de "suprimir, alterar o hacer inaccesible" ha permanecido inalterada. La razón por la cual se quiere disminuir esta conducta, es principalmente porque en nuestro idioma las acciones de borrar y suprimir apenas parecen diferenciables, mientras que el Consejo de Europa establece una disociación entre ambas, entendiendo "borrar" como la acción destruir los datos y "suprimir" como impedir o poner fin a la disposición de los mismos.

No obstante sí que se aprecia una importante diferencia entre el precepto recogido en el Código penal español y el que se encuentra en el Convenio: la necesidad de que las acciones recogidas tengan como consecuencia un resultado grave: "El que por cualquier medio, sin autorización y de manera grave borrase, dañase, deteriorase, alterase, suprimiese o hiciese inaccesibles datos informáticos, programas informáticos o documentos electrónicos ajenos, cuando el resultado producido fuera grave, será castigado con la pena de prisión de seis meses a tres años", es decir, para que este precepto pueda ser aplicado, se deberá causar un resultado grave tal y como se establece en el artículo 264.1 CP[26].

Además es necesario que las acciones sean realizadas a un sistema informático ajeno, entendiendo por ajeno no solo los pertenecientes a terceras personas, sino también los fabricados por uno mismo, pero vendidos a terceras personas habiéndose traspasado a un tercero la propiedad intelectual.

Junto a ellos encontramos el delito de interferencia del sistema tipificado en el artículo 5 del Convenio, cuyo objeto es obstaculizar grave, deliberada e ilegítimamente el funcionamiento de un sistema informático mediante diversas fórmulas entre las que se encuentran la introducción, supresión o alteración de datos informáticos. Esta conducta fue considerada por la Recomendación N (89) 9 como sabotaje informático y se caracteriza principalmente por la neutralidad de su lenguaje, permitiendo de este modo proteger los sistemas informáticos de todo tipo de obstáculo que impida el correcto funcionamiento.

Esta conducta ha sido ampliada por el artículo 264 bis del CP, donde el legislador español ha estimado pertinente especificar los posibles modos de cometer esta conducta: "A) realizando alguna de las conductas a que se refiere el artículo

[26]Concepto jurídica indeterminado sobre el que el legislador aún no se ha pronunciado

anterior, B) introduciendo o transmitiendo datos; o C) destruyendo, dañando, inutilizando, eliminando o sustituyendo un sistema informático, telemático o de almacenamiento de información electrónica", facilitando la labor a todo aquel que deba aplicar este tipo y evitando posibles confusiones con la conducta regulada en el artículo 4 del Convenio y 264 del CP. Concretamente, este delito trata de castigar conductas como el *mail bombing*, cuyo objeto es bloquear los servidores atacados a través de un masivo y simultáneo envío de correos electrónicos.[27]

Además, establece un agravante en el caso de que los perjudicados hubieran sido empresas, negocios o Administraciones públicas, pudiéndose alcanzar en tal caso la pena superior en grado.

Finalmente, este título se cierra con el artículo 6, en el que se recoge la conducta de abuso de los dispositivos. Este precepto determina como un delito plenamente independiente "la producción, venta, obtención para su utilización, importación, difusión u otra forma de puesta a disposición" de un tercero de cualquier dispositivo, contraseña o medio de acceso para poder cometer cualquier delito de los tipificados en los artículos 2 a 5 del Convenio, es decir, para poder acceder ilícitamente a un sistema informático, interferir ilícitamente en el mismo, atacar la integridad de los datos o atacar la integridad del sistema.

Esta disposición ha resultado un tanto polémica en España, al no haberse encontrado directamente recogida en el Código Penal hasta 2015, que fue introducida por el número 146 del artículo único de la L.O. 1/2015, de 30 de marzo, por la que se modifica la L.O. 10/1995, de 23 de noviembre, del Código Penal en el actual artículo 264 ter CP. En este caso, pese a castigar la misma conducta: la producción, adquisición o venta de sistemas informáticos para la comisión de determinados delitos, sí que se encuentran determinadas diferencias que en mi opinión deberían ser corregidas por el legislador, siendo la principal el delito que se va a cometer a través del medio producido, adquirido o vendido a tercero, puesto que el Convenio hace referencia a los delitos recogidos en el Título I del Capítulo II, es decir, acceso ilícito, interceptación ilícita, interferencia en los datos e interferencia en el sistema mientras que el legislador

[27]Es importante poner de relieve que, en el caso de que el *mail bombing* tuviese como finalidad obstruir u obstaculizar el orden público, convendría aplicarse el artículo 560.1 CP

español ha decidido disminuir el número de conductas a las dos reguladas en los artículos 264 (interferencia en el sistema) y 264 bis (interferencia en los datos) CP.

En conclusión, el precepto español está tipificando aquellas conductas cuya finalidad sea facilitar la comisión de los delitos regulados en los artículos 264 y 264 bis CP, sin tener en cuenta todas las conductas que realmente son apreciadas por el Convenio, y en consecuencia, sin castigar aquellas conductas que tengan por objeto facilitar los delitos de acceso ilícito e interceptación ilícita.

Además las consecuencias jurídicas derivadas de la comisión de este delito no se limitan al ámbito penal, sino que se amplían al ámbito civil donde puede exigirse indemnización relativa al lucro cesante conforme la interrupción y los daños causados, teniendo en cuenta aspectos como la duración de la interrupción, el tipo de actividad y las pérdidas en la cartera de clientes.

1.2. Los delitos informáticos

En segundo lugar, encontramos el título referido a *Los delitos informáticos*, contemplándose tan solo dos conductas: la falsificación y el fraude informático (artículos 7 y 8 del Convenio). Ambos son delitos relacionados con la manipulación de los sistemas y datos informáticos y considerados delitos medios[28], puesto que se realizan para poder cometer otros.

En primer lugar encontramos la falsificación informática (artículo 7), que consiste en "…la introducción, alteración, borrado o supresión de datos informáticos que dé lugar a datos no auténticos, con la intención de que sean tenidos en cuenta o utilizados a efectos legales como si se tratara de datos auténticos…". Con esta regulación se pretende establecer un delito paralelo al de falsificación de documentos tangibles.

---

[28] En el derecho penal se distinguen dos tipos de delitos, según se integre o no un resultado:

- Delitos de mera actividad: su realización se limita a una acción, sin que para su completa realización exija un resultado. Por ejemplo la mera intromisión en un sistema informático.
- Delitos de resultado: aquellos que para que se consideren realizados es necesaria una efectiva lesión del objeto, o al menos, que dicho objeto haya entrado en la radio de acción peligrosa.

Tanto los delitos de mera actividad como los delitos de resultado, pueden ser considerados delitos medio, siempre y cuando ellos se hayan realizado con la finalidad de poder cometer otro (delito final). Por ejemplo, la falsificación mediante medios informáticos de un documento, para poder tener acceso a una beca.

Fuente: SOLA RECHE, E., "El tipo de delito de acción doloso" en *Derecho penal. Parte General. Introducción teoría jurídica del delito*, ROMEO CASABONA *et al.* (coord.), Comares, 2013, p109.

Se trata de una conducta que no se encuentra expresamente regulada en nuestro Código Penal, donde en vez de establecer un tipo tan amplio y general como en el Convenio, se ha preferido incidir en los instrumentos falsificados, en su finalidad y en los sujetos infractores, distinguiendo entre particulares y funcionarios o autoridades públicas, todo ello regulado su Título XVIII. Esta es la razón por la cual no encontraremos un delito de falsificación informática como tal, sino que la falsedad de los documentos informáticos (también conocida como *spoofing*) se sancionará teniendo en cuenta dos aspectos: el soporte informático utilizado y el carácter del documento que representa por su fin social.

En esta materia, deberíamos tomar ejemplo de países como Francia, en cuya Ley 88/19 de 5 de Enero de 1988 sobre fraude informático contempla una serie de conductas como es el sabotaje informático referido a la falsificación de funcionamiento de un sistema informático, la destrucción de datos o la falsificación de documentos informatizados, sancionando a aquellas personas que falsifiquen documentos informatizados con intención de causar un perjuicio a otro. Junto a Francia, también cabe destacar la legislación alemana, en cuya Segunda Ley contra la Criminalidad Económica encontramos recogidos delitos como la alteración de datos informativos o el sabotaje informático, entendido como la destrucción, el deterioro, la eliminación o alteración de un sistema de datos.[29]

Este título del Convenio se cierra con el delito de fraude informático, entendido como aquellas conductas deliberadas e ilegítimas que tienen como finalidad causar un perjuicio patrimonial a través de los mecanismos descritos en el artículo. Con esta conducta, el legislador europeo pretende castigar a toda aquella persona que intente efectuar una manipulación indebida durante el procesamiento de datos, con una clara intención de realizar una transferencia ilegal de bienes. Además para asegurar la tipificación de todas las posibles manipulaciones de los datos informáticos el legislador no solo estableció las acciones más habituales para realizar este delito (introducir, alterar, borrar o suprimir datos informáticos), sino que añadió como cláusula de cierre la posibilidad de cometerlo mediante cualquier interferencia en el funcionamiento de un sistema informático, con intención fraudulenta o delictiva en aras a obtener ilegítimamente un beneficio económico.

[29] VIEGA RODRIGUEZ, M.J., *Un nuevo desafío jurídico: Los delitos informáticos*

Esta conducta, a diferencia de la falsificación informática, sí que la encontramos recogida en nuestra legislación, concretamente en el artículo 248 CP que tipifica la estafa informática, concebida como la obtención de lucro mediante un desplazamiento patrimonial sin consentimiento del propietario del patrimonio y realizada o bien a través de manipulaciones informáticas, o mediante engaños al sujeto pasivo. Además el legislador no se ha limitado a copiar el delito del Convenio, sino que ha extendido la sanción a todo aquel que fabrica, facilita, introduce o posee programas especializados para tal fin.

Por otra parte, no debemos olvidar el hecho de que la mayoría de las estafas informáticas son realizadas de forma masiva mediante el uso de programas informáticos que buscan el máximo número de víctimas posibles, por esta razón el legislador español ha previsto una serie de agravantes que se encuentran reguladas en el artículo 250 CP.

En conclusión, tal y como determina el Magistrado Don Eloy Velasco Nuñez[30], se trata de una asimilación para poder recoger y castigar exactamente con idéntica pena la estafa informática que la estafa sociológica[31]

1.3. Delitos relacionados con el contenido

En tercer lugar, se encuentran recogidos *Los delitos relacionados con el contenido*, en cuyo título únicamente se encuentra regulados los delitos relativos a la pornografía infantil. A efectos del Convenio, se considerará pornografía infantil, todo contenido pornográfico que contenga una representación visual de: A) un menor[32] comportándose de una forma sexualmente explícita, B) una persona mayor que aparezca con un menor comportándose de una forma sexualmente explícita, C) imágenes realistas que representan a un menor comportándose de una forma sexualmente explícita. En el

[30] ELOY VELASCO, E. "*Los delitos informáticos*". Diciembre 2015.
[31] Protocolo Facultativo de la Convención de las Naciones Unidas sobre los Derechos del Niño relativo a la venta de niños, la prostitución infantil y la utilización de niños en la pornografía La estafa sociológica es, según el Magistrado Don Eloy Velasco Nuñez, aquella que precisa del engaño a otro ser humano mediante cualquier fórmula de ingeniería social que, con cierta entidad, produciendo error en su víctima, de manera que le induzcan a realizar un acto de disposición con contenido económico no querido, en perjuicio propio o de tercero.
[32] Artículo 9.3 del Convenio: "(…) por «menor» se entenderá toda persona menor de dieciocho años. No obstante, cualquier Parte podrá establecer un límite de edad inferior, que será como mínimo de dieciséis años."

artículo 9 por lo tanto, se establece una enumeración[33] de conductas que los Estados parte deberán tipificar como delito en su derecho interno.

Esta disposición es consecuencia de la creciente necesidad de hacer frente a la producción, posesión y distribución informática de pornografía infantil, y responde a la preocupación por parte de los Jefes de Estado y de Gobierno del Consejo de Europa reflejada en su 21ª Cumbre (Estrasburgo, 10 a 11 de Octubre de 1997) en su Plan de Acción (punto III.4) [34] , paralela al actual objetivo internacional de prohibir la pornografía infantil.

En este aspecto debemos tener en cuenta el Protocolo Facultativo de la Convención de las Naciones Unidas sobre los Derechos del Niño relativo a la venta de niños, la prostitución infantil y la utilización de niños en la pornografía[35]. Este protocolo es un complemento de la Convención sobre los Derechos del Niño [36] y en él se desarrollan principalmente los artículos 34 y 35 de la misma, en los que se obliga a los gobiernos a proteger a los menores contra cualquier forma de explotación o abuso sexual, y a tomar todas las medidas posibles para erradicar el tráfico de menores.

Con esta disposición, el Consejo de Europa quiere reforzar las medidas de protección contra la explotación sexual de menores a través de la actualización de las disposiciones penales en el ámbito de los sistemas informáticos. Por ello no se limitan a castigar la tenencia de material pornográfico infantil, sino que además castigan la oferta o puesta a disposición, la difusión o transmisión y la adquisición mediante sistemas informáticos.

---

[33] Las conductas que deben ser tipificadas en el derecho interno como delito relacionado con la pornografía infantil son:

a. "La producción de pornografía infantil con vistas a su difusión por medio de un sistema informático;
b. la oferta o la puesta a disposición de pornografía infantil por medio de un sistema informático;
c. la difusión o transmisión de pornografía infantil por medio de un sistema informático,
d. la adquisición de pornografía infantil por medio de un sistema informático para uno mismo o para otra persona;
e. la posesión de pornografía infantil en un sistema informático o en un medio de almacenamiento de datos informáticos."

[34] Plan de Acción (punto III.4): https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016804e422a

[35] Protocolo Facultativo de la Convención de las Naciones Unidas sobre los Derechos del Niño relativo a la venta de niños, la prostitución infantil y la utilización de niños en la pornografía. UNICEF: http://www.unicef.org/spanish/specialsession/documentation/documents/op_se_sp.pdf

[36] Convención sobre los Derechos del Niño. BOE: https://www.boe.es/buscar/doc.php?id=BOE-A-1990-31312

En España, todas las conductas relacionadas con la pornografía infantil están tipificadas en nuestro Código, desde su elaboración hasta su difusión, favorecimiento o posesión del mismo. Concretamente se encuentran recogidas en el artículo 189 CP, donde se asimila la pornografía de menores de 18 años con la de personas con discapacidad aun cuando hayan superado la mayoría de edad.

Para redactar este delito, el legislador español optó por inspirarse en la Directiva 2011/92/UE del Parlamento Europeo y del Consejo de 13 de diciembre de 2011 relativa a la lucha contra los abusos sexuales y la explotación sexual de los menores y la pornografía infantil y por la que se sustituye la Decisión marco 2004/68/JAI del Consejo[37], en la que se define pornografía infantil como todo aquel material en el que participa un menor o discapacitado en una conducta sexual explícita, o la representación de sus órganos sexuales con fin principalmente sexual. Este debe concepto debe completarse con la sentencia del Tribunal Supremo de 8 de marzo de 2006 donde se determina que, en definitiva, "la pornografía infantil exige: la existencia de un menor de edad real y la de actos, imágenes o posturas no neutrales sexualmente, de modo que haya una acción sexuada ajena al propio menor y descartando el simple desnudo, la pornografía escrita y la oral, porque está siempre debe ser visual". Esto pone en duda la punibilidad de la ya conocida pornografía virtual y técnica: dibujos caracterizados por su alto nivel de realismo y en los que aparecen menores en posturas de índole sexual. Se trata entonces, de un debate actualmente abierto entre, por una parte, los que apoyan el hecho de castigar este tipo de pornografía, y, por otra, los opinan que en tal caso, se estaría llegando al extremo de tipificar conductas más amorales que penales, puesto que lo que se pretende proteger jurídicamente, con la conducta regulada en el artículo 189 CP, es el crecimiento armónico de la sexualidad del menor, y, a través de la realización de unos determinados dibujos o imágenes ficticias no habría sujeto pasivo, y en consecuencia, no se estaría causando perjuicio alguno a menores.

No obstante, la legislación española sí que ofrece una serie de agravantes para determinados supuestos como el caso de que la edad del menor sea inferior a 16 años, revestir los hechos de un carácter especialmente degradante o vejatorio, que se contextualice en un entorno de violencia física o sexual, que se ponga en peligro la vida

[37]Directiva 2011/92/UE del Parlamento Europeo y del Consejo de 13 de diciembre de 2011 relativa a la lucha contra los abusos sexuales y la explotación sexual de los menores y la pornografía infantil y por la que se sustituye la Decisión marco 2004/68/JAI del Consejo. BOE: https://www.boe.es/doue/2011/335/L00001-00014.pdf

de la víctima o que estas conductas se realicen en el seno de una organización dedicada a la producción o distribución de material pornográfico.

Además, en el octavo precepto de este artículo se faculta al Juez o Ministerio Fiscal a retirar/bloquear el acceso a aquellas páginas web o aplicaciones que contengan, permitan la difusión o elaboren pornografía infantil[38]. Todo ello, con la finalidad de permitir y asegurar un desarrollo normal de la madurez sexual del menor, protegiendo así su inocencia y pureza.

1.4. Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines.

La comisión de delitos contra la propiedad intelectual es uno de los delitos más comunes realizados a través de Internet. Entre ellos se encuentran la reproducción y difusión de obras (literarias, musicales, audiovisuales…).

Con la finalidad de poder poner fin a estas conductas, el legislador europeo estimó conveniente incluir un delito cuyo bien jurídico protegido fuese la propiedad intelectual, disponiendo sanciones penales y aumentando la cooperación internacional en esta materia.

Concretamente, se recoge en el Titulo cuarto de este primer capítulo la última conducta delictiva: los delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines (artículo 10 del Convenio), donde se establece que cada Estado parte adoptará las medidas legislativas y de otro tipo que resulten necesarias, para tipificar con delito en su normativa interna las infracciones de la propiedad intelectual, según se definan en sus legislaciones internas, de conformidad con las obligaciones asumidas en el Acta de París de 24 de julio de 1971 por la que se revisó el Convenio de Berna para la protección de obras literarias y artísticas[39], del Acuerdo sobre los aspectos de los derechos de la propiedad intelectual relacionados con el comercio[40] y del Tratado de la Organización Mundial de la Propiedad Intelectual (OMPI) sobre la Interpretación

[38] Artículo 13 Ley Enjuiciamiento Criminal, permite en este sentido solicitar al juez el cierre o bloqueo de una página web que contenga, distribuya o elabore pornografía infantil.
[39]Convenio Berna para la protección de obras literarias y artísticas. Fuente: http://www.wipo.int/treaties/es/text.jsp?file_id=283700
[40]Acuerdo sobre los aspectos de los derechos de la propiedad intelectual relacionados con el comercio: http://www.wipo.int/treaties/es/text.jsp?file_id=305906

o Ejecución y Fonogramas[41]. La observancia de estos dos últimos textos normativos tuvo una relevante trascendencia, puesto que se trataba de textos que en el momento de la celebración del Convenio, aún no habían entrado en vigor y, en consecuencia, al entrar en vigor actualizaron considerablemente la protección de la propiedad intelectual a nivel internacional.

En conclusión, los Estados miembro deben tipificar las conductas conforme a estos textos internacionales, considerando las obligaciones que hayan contraído respecto de dichos textos, pero ello no impide que las definiciones de estos delitos varíen dependiendo de la legislación nacional de cada Estado. En este aspecto debemos prestar especial atención, puesto que la única infracción recogida en el Convenio sobre Ciberdelincuencia es la relativa a la propiedad intelectual, quedando fuera de este modo infracciones en materia de patentes o de marcas comerciales.

Nuestra legislación recoge las consecuencias penales de estas conductas en los artículos 270-273 CP, pero ello no indica que sean las únicas consecuencias jurídicas que el ordenamiento español haya previsto para delitos contra la propiedad intelectual. Con ello me refiero a tratamientos alternativos como pueden ser los establecidos en el Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual[42] en su Libro III denominado *Protección de los derechos recogidos en esta ley*, donde se observan medidas como el cese de la actividad ilícita, indemnizaciones y medidas cautelares entre otros. Luego los castigos establecidos en nuestro Código no siempre son de aplicación cuando se realiza una conducta que daña la propiedad intelectual, sobre todo teniendo en cuenta las elevadas penas privativas de libertad previstas.

Las conductas que son tipificadas por el Derecho penal se caracterizan por tener una entidad masiva y ánimo de lucro. En concreto, el delito básico regulado en el artículo 270 CP castiga a aquella persona que, con intención de lucrarse económicamente y en perjuicio de tercero, reproduzca, plagie, distribuya, comunique o explote públicamente, en todo o en parte, una obra artística, literaria o científica, sin autorización de los titulares de derechos de la propiedad intelectual. En este delito lo

[41] Tratado de la Organización Mundial de la Propiedad Intelectual (OMPI) sobre la Interpretación o Ejecución y Fonogramas: www.wipo.int/edocs/mdocs/diplconf/es/crnr_dc/crnr_dc_95_rev.doc

[42] Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual. BOE: https://www.boe.es/buscar/act.php?id=BOE-A-1996-8930&p=20141105&tn=2

que se quiere castigar es la deslealtad de quien se beneficia económicamente en perjuicio de tercero. En lo que a este trabajo respecta, el apartado 2 del artículo 270 CP adquiere una especial importancia ya que hace referencia a quien facilite el acceso o la localización en internet de obras o prestaciones objeto de propiedad intelectual sin la autorización de los correspondientes titulares, considerando la posibilidad de bloquear el acceso a dicho portal de Internet. Se trata de una consecuencia o medida cautelar cada vez más empleada por los Tribunales de nuestro país. En este sentido se declaró un Juez de Elche en diciembre de 2014 al ordenar el bloqueo cautelar del acceso a los sitios web de enlaces a descargas Películas Pepito y Series Pepito[43].

En la actualidad, los portales de Internet que nos facilitan el acceso a determinadas obras, películas e incluso programas informáticos están comenzando a desaparecer, pero ello no indica que no se deba continuar legislando en esta materia, e incluso, endurecer las penas teniendo en cuenta el objeto de protección del presente delito, es decir, la propiedad intelectual y la amenaza que Internet le supone.

2. DERECHO PROCESAL Y COOPERACIÓN INTERNACIONAL

El legislador del Convenio, teniendo en cuenta las recomendaciones de otros instrumentos internacionales relativos a la cibercriminalidad, decidió establecer en su tercer capítulo una regulación relativa a los sistemas de cooperación internacional para poder hacer frente a la ciberdelincuencia. No obstante, este apartado no debe analizarse individualmente, sino que debe ponerse en relación con el Derecho procesal y la jurisdicción (secciones segunda y tercera del primer capítulo). Esto es así, porque el Derecho procesal es uno de los aspectos más relevantes del Convenio. Concretamente, mediante el artículo 15 de este Convenio se obliga a los Estados parte a que se doten de los poderes y procedimientos necesarios para poder alcanzar los objetivos de las investigaciones o procesos penales, respetando todos los textos internacionales relativos a los derechos fundamentales, haciendo especial hincapié en los recogidos en el Convenio del Consejo de Europa para la protección de los derechos humanos y las libertades fundamentales (1950)[44], del Pacto Internacional de derechos civiles y

[43] Noticia del cierre del acceso facilitado por las páginas web Películas Pepito y Series Pepito. El mundo: http://www.elmundo.es/tecnologia/2014/12/03/547f1edae2704edf458b45a1.html
[44]Convenio del Consejo de Europa para la protección de los derechos humanos y las libertades fundamentales. BOE: https://www.boe.es/buscar/doc.php?id=BOE-A-1979-24010

políticos de las Naciones Unidas (1966)[45], y de otros instrumentos internacionales aplicable en materia de derechos humanos.

Entre todas las obligaciones que han sido impuestas a través del Convenio, debemos enfatizar la recogida en el artículo 16, que establece que los Estados miembros, deberán permitir a sus autoridades competentes ordenar o imponer la conservación rápida de determinados datos electrónicos que forman parte de una investigación o procedimiento penal específico (incluyendo los datos sobre el tráfico) almacenados por medio de un sistema informático, especialmente cuando se trate de datos susceptibles de pérdidas o de modificación. No obstante, esta medida no implica que los Estados miembros restrinjan la oferta o el uso de determinados servicios que no puedan recopilar o conservar ciertos datos.

El segundo apartado de este mismo precepto, impone a los Estados parte la obligación de establecer las medidas legislativas necesarias para que de nuevo, las autoridades competentes puedan ordenar la conservación y protección de la integridad de determinados datos informáticos, durante el tiempo necesario (hasta un máximo de 90 días) a una persona. Concretamente el Convenio establece "a esa persona", refiriéndose con ello al sujeto que tenga en posesión o bajo control dichos datos.

Este precepto debe relacionarse con lo establecido en el artículo 29 del Convenio en materia de cooperación y asistencia mutua, el cual determina que se podrá solicitar a otro Estado parte que ordene o asegure la conservación rápida de datos almacenados por medio de un sistema informático que se encuentre en su territorio. Para ello, el Estado que realice el requerimiento deberá proceder conforme lo establecido en el artículo 29 del Convenio en sus apartados 2 y 3.

Llegados a este punto, debe tenerse en cuenta que las "autoridades" a las que el Convenio está haciendo referencia, deben ser obligatoriamente autoridades judiciales. Así lo ha determinado la doctrina mayoritaria española, que encuentra el fundamento de esta idea en el artículo 18.3 de la Constitución Española (CE a partir de ahora), el cual garantiza el secreto de las comunicaciones salvo resolución judicial. Por lo tanto, el hecho de que una autoridad no judicial ordene la conservación de determinados datos

[45]Pacto Internacional de derechos civiles y políticos de las Naciones Unidas: BOE: https://www.boe.es/diario_boe/txt.php?id=BOE-A-1977-10733

almacenados en un soporte informático, vulnera el derecho fundamental al secreto de las comunicaciones.

Paralelamente, tiene gran importancia una sentencia del Tribunal Constitucional previa al Convenio sobre la Ciberdelincuencia: la STC 114/84, en la que se manifiesta que el secreto de las comunicaciones pretende proteger a los interlocutores de una comunicación, de intromisiones de terceras personas, es decir, tal y como establece dicha sentencia "garantiza que nadie ajeno al emisor y al receptor de la comunicación entre en conocimiento del contenido de la misma sin la autorización de los comunicantes. Se trata pues de un derecho que obliga a terceros, pero jamás a los propios participes en la comunicación". Pero ello no indica que uno de los interlocutores no pueda informar o, en nuestro caso, almacenar conversaciones o contenidos que puedan determinar la comisión de un delito o ser esenciales para una investigación penal. Concretamente, la sentencia determina que el artículo 18.3 CE "no puede oponerse, sin quebrar su sentido constitucional, frente a quien tomó parte en la comunicación misma así protegida. Rectamente entendido, el derecho fundamental consagra la libertad de las comunicaciones".

En conclusión, el hecho de una autoridad judicial ordene la conservación de unos determinados datos a la persona que la posea, ya sean propios o información que una persona le ha transmitido directamente, no vulnera la garantía del secreto de las comunicaciones recogida en el artículo 18.3 CE.

No obstante, también debemos tener en cuenta que existen una serie de causas por las que el Estado requerido podrá denegar las solicitudes de conservación de datos (artículo 29.4 y 29.5 del Convenio). En primer lugar, puede darse la situación de que un Estado requiera la doble tipificación penal como condición *sine qua non* para aceptar la solicitud de asistencia mutua en investigaciones penales o delitos distintos de los recogidos en los artículos 2 a 11 del Convenio. En los restantes casos, las solicitudes de cooperación únicamente podrá denegarse bien, si la solicitud hace referencia a un delito que el Estado requerido considera delito político[46] o bien, cuando el Estado requerido

[46] Delito político: aquel que tiene como objeto único y exclusivo, destruir, cambiar o perturbar el orden público.
BOE: http://www.enciclopedia-juridica.biz14.com/d/delitos-pol%C3%ADticos-y-conexos/delitos-pol%C3%ADticos-y-conexos.htm

considere que la ejecución de la solicitud podría atentar contra su soberanía, seguridad, orden público u otros intereses esenciales.

En lo que a ámbito de cooperación y derecho procesal se refiere, también es importante resaltar que el Convenio prevé en su artículo 20 que los Estados parte puedan adoptar medidas necesarias para facultar a sus autoridades competentes la solicitud de registro y confiscación de datos informáticos almacenados, la obtención en tiempo real sobre el tráfico y la interceptación de datos sobre el contenido de determinados documentos. La mayoría de los Estados parte limitan este poder de interceptación a una serie de delitos graves, puesto que este poder de los Estados colisiona con nuestro derecho a la privacidad de las telecomunicaciones. En el caso de España, la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones (Ley 25/2007 a partir de ahora)[47] trata de precisar la obligación de los operadores[48] de conservar aquellos datos generados o tratados en el marco de prestación de servicios de comunicaciones electrónicas tal y como indica en su artículo 1.

En su preámbulo se define como una norma realizada para proteger la seguridad pública, teniendo en cuenta todos los derechos individuales que pueden verse afectados, como son los relativos a la intimidad de las comunicaciones y la privacidad. Por esta razón, el legislador español creyó conveniente concretar en el artículo 3 de la Ley 25/2007 qué datos son objeto de conservación entre los que se encuentran los relativos a facilitar la identificación del origen de una comunicación, el destino de la misma, el momento en que se produce o la localización del equipo de comunicación móvil. Finalmente, esta ley determina el modo en que debe conservarse dicha información y en que debe proceder a su cesión.

En último lugar, para finalizar este apartado relativo al derecho procesal y cooperación internacional, debemos hacer alusión a la posibilidad que el Convenio ofrece a aquellos Estados que no puedan otorgar a sus autoridades competentes la facultad de realizar las medidas descritas en el apartado primero del artículo 20 relativas a la obtención en tiempo real de datos sobre el tráfico como consecuencia de los

[47] Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones. BOE: https://www.boe.es/buscar/doc.php?id=BOE-A-2007-18243

[48] En el artículo 2 de la Ley 25/2007 define operadores como los sujetos que presenten servicios de comunicaciones electrónicas disponibles al público o exploten redes públicas de comunicaciones.

principios fundamentales de su ordenamiento jurídico interno, concediéndoles la posibilidad de tomar las medidas legislativas y de otro tipo que resulten necesarias para asegurar la obtención en tiempo real de los datos sobre el tráfico.

3. ÁMBITO JURISDICCIONAL Y ASISTENCIA MUTUA

La competencia jurisdiccional se encuentra determinada en el Convenio por el artículo 22, en el cual se establece el principio de territorialidad. Concretamente determina que cada Estado miembro deberá adoptar las medidas legislativas y de otro tipo que fuesen necesarias para afirmar su jurisdicción respecto de los delitos previstos en el Convenio que hayan sido cometidos en su territorio. No obstante, este principio es complementado para los casos en los que el delito se cometa a bordo de un buque -en cuyo caso será competente el Estado parte cuyo pabellón enarbole- o una aeronave -donde deberemos atender conforme a qué leyes ha sido matriculada dicha aeronave-.

Junto a ello debe ponerse de relieve la cláusula de cierre de este precepto, puesto que en el caso de que un sujeto nacional de un Estado miembro, cometa uno de los delitos regulados en el Convenio de modo que ningún Estado tenga competencia territorial sobre el mismo o cuando dicha conducta sea susceptible de sanción penal en el Estado en el que se cometió, el Estado miembro del que sea nacional tendrá competencia para conocer del asunto. En tal caso, resultaría esencial poner en práctica el procedimiento de extradición que se encuentra regulado en el artículo 24 del Convenio.

Llegados a este punto, debemos ser conscientes de que dicho procedimiento puede encontrarse condicionado a la existencia de tratados o convenios específicos de extradición o entrega de la persona, causando un grave problema en caso de que un Estado miembro que exija un tratado de extradición, reciba una solicitud de un Estado con el que no tiene ningún acuerdo. Esta situación fue prevista por el legislador europeo, quien introdujo una solución a esta posible dificultad en el artículo 24.3 del Convenio, determinando que ante tal situación podrá aplicarse el Convenio sobre la Ciberdelicuencia como fundamento jurídico de la extradición relativa a los delitos regulado en los artículos 2 a 11 del presente texto normativo.

Este precepto se encuentra estrechamente vinculado con el artículo 25 del Convenio, que regula tal y como indica en su primer apartado, la "asistencia mutua para los fines de las investigaciones o procedimientos relativos a los delitos relacionado con sistemas y datos informáticos". Según el Informe explicativo del Convenio, la asistencia mutua ha de ser amplia y no debe limitarse a los delitos penales relacionados con sistemas y datos informáticos, sino que también deberá prestarse en lo relativo a obtención de pruebas en formato electrónico de una de las conductas recogidas.

La asistencia mutua es, desde mi punto de vista, algo esencial para la lucha contra la ciberdelincuencia. Esto es así debido a la gran libertad territorial que Internet concede al infractor para cometer delitos, llegando incluso al extremo de no saber dónde puede hallarse el sujeto activo.

V. CONCLUSIONES

Con la finalidad de aplicar una política penal común para proteger a la sociedad de la ciberdelincuencia, el Convenio consigue una cooperación internacional reforzando la materia penal interna de los Estados y haciendo la aplicación de la ley más eficaz, rápida y fiable para los Estados miembros.

Junto a ello, consigue solventar la problemática de la disociación entre el lugar desde el cual se causa el daño y el lugar donde se localiza el resultado de ese daño, efecto de la inexistencia de barreras físicas que permiten la libre circulación de la información a través de Internet. Así, nace la necesidad de cooperación entre diferentes países para poder zanjar un mismo problema.

Por lo tanto, podríamos considerar un objetivo prioritario el aumento de número de Estados parte del Convenio. Esto permitiría la posibilidad real de obtener resultados concluyentes cuando los ciberdelitos se cometan en el ámbito internacional y todos los países afectados sean parte del Convenio.

En esta ocasión España es un referente en la suscripción del Convenio. No obstante, siendo críticos, podríamos recriminar la no inclusión en detalle de todos los delitos recogidos en el Convenio aunque si lo haga de manera general. Con ello me refiero a aquellas ocasiones en las que el legislador español ha decidido no incluir todos

los modos de cometer la conducta que han sido determinados en el Convenio, disminuyendo así, las posibles vías de identificar un delito. Un ejemplo de ello sería la regulación establecida en el artículo 6 del Convenio respecto de la producción, venta, obtención para su utilización, importación, difusión u otra forma de puesta a disposición de cualquier dispositivo para poder cometer un delito de los recogidos en los artículo 2 a 5 del Convenio. Aquí el legislador español, en vez de hacer referencia a los delitos recogidos en los artículos 2 a 5 del Convenio, o directamente nombrarlos, ha decidido disminuir el número de conductas a dos: interferencia en el sistema e interferencia en los datos, de tal manera que, acatando el tenor literal de la norma, si un sujeto vende un dispositivo a un tercero para que éste acceda ilícitamente a un sistema informático, la persona que ha vendido dicho dispositivo no sería castigada, o al menos, no sería castigada conforme al artículo 264 ter CP, que es el que recoge esta conducta.

Además también debemos poner de relieve la inexistencia de regulación de la falsificación informática, conducta que, como ya se ha puesto de relieve, no se encuentra expresamente regulada en nuestro Código Penal.

Como última objeción por mi parte, me gustaría subrayar la necesidad de introducir en nuestro Código Penal, un capítulo cuyo objeto sea la ciberdelincuencia, en el cual se establezcan todos los delitos que se pueden cometer a través de un sistema informático.

En conclusión podríamos decir que el Convenio sobre ciberdelincuencia es un texto referente en la materia. Pero ello, no indica que se deba dejar de legislar sobre la misma, sino que conforme se vaya desarrollando las nuevas tecnologías, paralelamente, deberemos incidir en su regulación.

VI. BIBLIOGRAFÍA

1. OBRAS GENERALES Y MONOGRAFÍAS

- SOLA RECHE, E., *Derecho penal. Parte General. Introducción teoría jurídica del delito*, ROMEO CASABONA *et al.* (coord.), 2013, Comares.
- JIMÉNEZ GARCÍA, F., *La protección y seguridad de la persona en internet: aspectos sociales y jurídicos*, JORDA CAPITAN E. R., et al.(coord.), 2014, Scientia Iuridica.
- MANGAS MARTÍN, A., *Instituciones y Derecho de la Unión Europea*, sexta edición, 2014, Tecnos.

2. ARTÍCULOS DE REVISTAS Y CAPÍTULOS DE LIBROS

- AGUIRRE ROMERO, J. "Ciberespacio y comunicación: nuevas formas de vertebración social en el siglo XXI" en *Revista de estudios literarios*. Universidad Complutense de Madrid, 2004.
- ANARTE BORRALLO, E., "Incidencia de las nuevas tecnologías en el sistema penal. Aproximación al Derecho pena en la sociedad de la información" en *Derecho y conocimiento*, págs. 191-257.
- BALLESTEROS TEJADO, E, "Europa se refuerza penalmente frente a los ataques a los sistemas de información" en *Ciberseguridad, seguridad de la información y privacidad,* Nº. 107, 2013, págs. 92-94.
- BARRIO ANDRÉS, M. "La ciberdelincuencia en el Derecho español" en *Revista de las Cortes Generales*, Nº 83, 2011, págs. 273-305.
- DE DIOS MESEGUER GONZALEZ, J., "Los nuevos modi operandi de los ciberdelincuentes durante la crisis económica" en *Revista de Derecho UNED*, Nº 12, 2013.
- DEL CERRO ESTEBAN, J.A., "La adaptación del sistema penal español al Convenio sobre ciberdelincuencia en materia de pornografía infantil", en *Estudios jurídicos*, Nº. 2012, 2012.
- DÍAZ GÓMEZ A., "El delito informático, su problemática y la cooperación internacional como paradigma de su solución: El Convenio de Budapest" en *REDUR*, diciembre 2010, págs. 169-203.

- ELOY VELASCO, E. “Los delitos informáticos”. Artículo monográfico. Diciembre 2015.
- GONZALEZ HURTADO, J.A., “Delincuencia informática: Daños informáticos del artículo 264 del Código Penal y propuesta de reforma”, Universidad Complutense de Madrid, Madrid, 2013.
- GUTIÉRREZ FRANCÉS, M.L., “Reflexiones sobre la Ciberdelincuencia hoy”, *REDUR 3*, 2005, págs. 209-234.
- RAYÓN BALLESTEROS, M. A., “Cibercrimen: particularidades en su investigación y enjuiciamiento”, en *Anuario Jurídico y Económico Escurialense*, nº XLVII, 2014.
- RODRIGUEZ BERNAL, A. “Los Cibercrímenes en el Espacio de Libertad, Seguridad y Justicia” en *Revista de derecho informático*, nº 103, 2007.

3. WEBGRAFÍA:

(Todas direcciones electrónicas siguientes han sido consultadas por última vez el 1 de junio de 2016)

- Acuerdo sobre los aspectos de los derechos de la propiedad intelectual relacionados con el comercio: http://www.wipo.int/treaties/es/text.jsp?file_id=305906
- Código penal español: BOE: https://www.boe.es/buscar/act.php?id=BOE-A-1995-25444
- Consejo de Europa: http://www.coe.int/en/web/portal/home
- Convenio Berna para la protección de obras literarias y artísticas: http://www.wipo.int/treaties/es/text.jsp?file_id=283700
- Convención sobre los Derechos del Niño: BOE: https://www.boe.es/buscar/doc.php?id=BOE-A-1990-31312
- Convención Europea de Derechos Humanos: http://www.echr.coe.int/Documents/Convention_SPA.pdf
- Convenio sobre Ciberdelincuencia: BOE: http://www.boe.es/diario_boe/txt.php?id=BOE-A-2015-793
- Directiva 2011/92/UE del Parlamento Europeo y del Consejo de 13 de diciembre de 2011 relativa a la lucha contra los abusos sexuales y la explotación sexual de los menores y la pornografía infantil: BOE: https://www.boe.es/doue/2011/335/L00001-00014.pdf

- Informe explicativo del Convenio: https://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/ETS%20185%20Explanatory%20report_Spanish.pdf
- Instrumento de ratificación: BOE: https://www.boe.es/diario_boe/txt.php?id=BOE-A-2010-14221
- L.O. 1/2015, de 30 de marzo, por la que se modifica la L.O. 10/1995, de 23 de noviembre, del Código Penal: BOE: https://www.boe.es/diario_boe/txt.php?id=BOE-A-2015-3439
- Noticia del cierre del acceso facilitado por las páginas web Películas Pepito y Series Pepito: http://www.elmundo.es/tecnologia/2014/12/03/547f1edae2704edf458b45a1.html
- Plan de Acción (punto III.4): https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016804e422a
- Protocolo adicional: BOE: https://www.boe.es/diario_boe/txt.php?id=BOE-A-2015-793
- Protocolo Facultativo de la Convención de las Naciones Unidas sobre los Derechos del Niño relativo a la venta de niños, la prostitución infantil y la utilización de niños en la pornografía: http://www.unicef.org/spanish/specialsession/documentation/documents/op_se_sp.pdf
- Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual: BOE: https://www.boe.es/buscar/act.php?id=BOE-A-1996-8930&p=20141105&tn=2
- Tabla de Estados Miembros del Convenio sobre Ciberdelincuencia: http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures
- Tratado de la Organización Mundial de la Propiedad Intelectual (OMPI) sobre la Interpretación o Ejecución y Fonogramas: www.wipo.int/edocs/mdocs/diplconf/es/crnr_dc/crnr_dc_95_rev.doc
- Unión Europea: http://europa.eu/index_es.htm

VII. ANEXOS

Anexo I: Estados parte del Convenio de Ciberdelincuencia miembros del Consejo de Europa:

Members of Council of Europe										
	Signature	**Ratification**	**Entry into Force**	**Notes**	**R.**	**D.**	**A.**	**T.**	**C.**	**O.**
Albania	23/11/2001	20/06/2002	01/07/2004				A.			
Andorra	23/04/2013									
Armenia	23/11/2001	12/10/2006	01/02/2007				A.			
Austria	23/11/2001	13/06/2012	01/10/2012		R.	D.	A.			
Azerbaijan	30/06/2008	15/03/2010	01/07/2010		R.	D.	A.	T.		
Belgium	23/11/2001	20/08/2012	01/12/2012		R.	D.	A.			
Bosnia and Herzegovina	09/02/2005	19/05/2006	01/09/2006				A.			
Bulgaria	23/11/2001	07/04/2005	01/08/2005		R.	D.	A.			
Croatia	23/11/2001	17/10/2002	01/07/2004				A.			
Cyprus	23/11/2001	19/01/2005	01/05/2005				A.			
Czech Republic	09/02/2005	22/08/2013	01/12/2013		R.	D.	A.			
Denmark	22/04/2003	21/06/2005	01/10/2005		R.		A.	T.		
Estonia	23/11/2001	12/05/2003	01/07/2004				A.			
Finland	23/11/2001	24/05/2007	01/09/2007		R.	D.	A.			
France	23/11/2001	10/01/2006	01/05/2006		R.	D.	A.			
Georgia	01/04/2008	06/06/2012	01/10/2012			D.				
Germany	23/11/2001	09/03/2009	01/07/2009		R.	D.	A.			
Greece	23/11/2001									
Hungary	23/11/2001	04/12/2003	01/07/2004		R.	D.	A.			
Iceland	30/11/2001	29/01/2007	01/05/2007		R.		A.			
Ireland	28/02/2002									
Italy	23/11/2001	05/06/2008	01/10/2008				A.			
Latvia	05/05/2004	14/02/2007	01/06/2007		R.		A.			
Liechtenstein	17/11/2008	27/01/2016	01/05/2016		R.	D.	A.			
Lithuania	23/06/2003	18/03/2004	01/07/2004		R.	D.	A.			
Luxembourg	28/01/2003	16/10/2014	01/02/2015				A.			
Malta	17/01/2002	12/04/2012	01/08/2012			D.				
Moldova	23/11/2001	12/05/2009	01/09/2009			D.	A.	T.		
Monaco	02/05/2013									
Montenegro	07/04/2005	03/03/2010	01/07/2010	55	R.		A.			

Netherlands	23/11/2001	16/11/2006	01/03/2007				A.	T.		
Norway	23/11/2001	30/06/2006	01/10/2006		R.	D.	A.			
Poland	23/11/2001	20/02/2015	01/06/2015		R.		A.			
Portugal	23/11/2001	24/03/2010	01/07/2010			D.	A.			
Romania	23/11/2001	12/05/2004	01/09/2004				A.			
Russia										
San Marino										
Serbia	07/04/2005	14/04/2009	01/08/2009	55			A.			
Slovakia	04/02/2005	08/01/2008	01/05/2008		R.	D.	A.			
Slovenia	24/07/2002	08/09/2004	01/01/2005				A.			
Spain	23/11/2001	03/06/2010	01/10/2010			D.	A.			
Sweden	23/11/2001									
Switzerland	23/11/2001	21/09/2011	01/01/2012		R.	D.	A.			
The former Yugoslav Republic of Macedonia	23/11/2001	15/09/2004	01/01/2005				A.			
Turkey	10/11/2010	29/09/2014	01/01/2015							
Ukraine	23/11/2001	10/03/2006	01/07/2006		R.	D.	A.			
United Kingdom	23/11/2001	25/05/2011	01/09/2011		R.		A.			

R.: Reservations D.: Declarations A.: Authorities T.: Territorial Application C.: Communication O.: Objection.

Anexo II: Estados parte del Convenio de Ciberdelincuencia no miembros del Consejo de Europa:

Non-Members of Council of Europe										
	Signature	**Ratification**	**Entry into Force**	**Notes**	**R.**	**D.**	**A.**	**T.**	**C.**	**O.**
Argentina										
Australia		30/11/2012 a	01/03/2013		R.		A.			
Canada	23/11/2001	08/07/2015	01/11/2015		R.	D.	A.			
Chile										
Colombia										
Costa Rica										
Dominican Republic		07/02/2013 a	01/06/2013			D.	A.			

Israel		09/05/2016 a	01/09/2016		R.		A.			
Japan	23/11/2001	03/07/2012	01/11/2012		R.	D.	A.			
Mauritius		15/11/2013 a	01/03/2014				A.			
Mexico										
Morocco										
Panama		05/03/2014 a	01/07/2014				A.			
Paraguay										
Peru										
Philippines										
Senegal										
South Africa	23/11/2001									
Sri Lanka		29/05/2015 a	01/09/2015		R.	D.	A.			
Tonga										
United States of America	23/11/2001	29/09/2006	01/01/2007		R.	D.	A.			
Total number of signatures not followed by ratifications	6									
Total number of ratifications/accessions	49									

R.: Reservations D.: Declarations A.: Authorities T.: Territorial Application C.: Communication O.: Objection.